



Appendix E: Attestation of Compliance – Service Providers
**Payment Card Industry (PCI)
Data Security Standard**

**Attestation of Compliance for
Onsite Assessments – Service Providers**

Version 1.2.1

July 2009

Instructions for Submission

The Qualified Security Assessor (QSA) and Service Provider must complete this document as a declaration of the Service Provider's compliance status with the Payment Card Industry Data Security Standard (PCI DSS). Complete all applicable sections and submit to the requesting payment brand.

Part 1. Qualified Security Assessor Company Information

Company Name: CQR Consulting Pty Ltd
 Lead QSA Contact Name: Phil Kernick Title: Information Security Professional
 Telephone: +61883645881 E-mail: phil.kernick@cqrconsulting.com
 Business Address: 196 Fullarton Rd City: Dulwich
 State/Province: SA Country: Australia ZIP: 5065
 URL: http://www.cqrconsulting.com/

Part 2. Service Provider Organization Information

Company Name: Our Community Foundation DBA(s): Our Community Foundation
 Contact Name: Denis Moriarty Title: Group Managing Director
 Telephone: +61393206812 E-mail: DenisM@ourcommunity.com.au
 Business Address: 51 Stanley Street City: West Melbourne
 State/Province: VIC Country: Australia ZIP: 3003
 URL: http://www.ourcommunity.com.au

Part 2a. Services Provided (check all that apply)

- Authorization Loyalty Programs 3-D Secure Access Control Server
 Switching IPSP (E-commerce) Process Magnetic-Stripe Transactions
 Payment Gateway Clearing & Settlement Process MO/TO Transactions
 Hosting Issuing Processing Others (please specify): Our Community Foundation provides payment processing services for not-for-profit organisations using Our Community Foundation's merchant account. Transactions are acquired from cardholders through online channels. However, within Our Community Foundation's payment application, all payment processing functionality is outsourced to a payment service provider (Qvalent - a subsidiary of Westpac Banking Corporation).

List facilities and locations included in PCI DSS review: All storage, processing and transmission facilities located at 51 Stanley St West Melbourne, and the outsourced environment hosted by Qvalent.

Part 2b. Relationships

Does your company have a relationship with one or more third-party service providers (for example, gateways, web-hosting companies, airline booking agents, loyalty program agents, etc)? Yes No

Part 2c. Transaction Processing

How and in what capacity does your business store, process and/or transmit cardholder data? Our Community Foundation provides payment processing services for not-for-profit organisations using Our Community Foundation's merchant account. Transactions are acquired from cardholders through

online channels. However, within Our Community Foundation's payment application, all payment processing functionality is outsourced to a payment service provider (Qvalent - a subsidiary of Westpac Banking Corporation).

Payment Application in use: *Developed In-House*

Payment Application Version:



Part 3. PCI DSS Validation

Based on the results noted in the Report on Compliance ("ROC") dated 01/Jun/2011, Phil Kernick asserts the following compliance status for the entity identified in Part 2 of this document as of 01/Jun/2011 (check one):

Compliant: All requirements in the ROC are marked "in place¹," and a passing scan has been completed by the PCI SSC Approved Scanning Vendor *McAfee* thereby *Our Community Foundation* has demonstrated full compliance with the PCI DSS 1.2.

Non-Compliant: Some requirements in the ROC are marked "not in place," resulting in an overall **NON-COMPLIANT** rating, or a passing scan has not been completed by a PCI SSC Approved Scanning Vendor, thereby (*Service Provider Name*) has not demonstrated full compliance with the PCI DSS.

Target Date for Compliance:

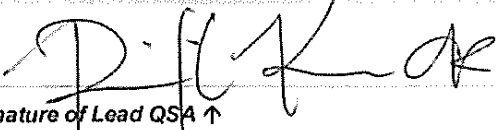
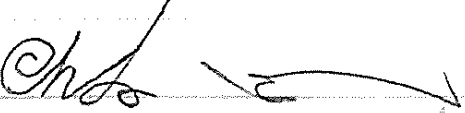
An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with the payment brand(s) before completing Part 4, since not all payment brands require this section.*

Part 3a. Confirmation of Compliant Status

QSA and Service Provider confirm:

- The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures, Version 1.2*, and was completed according to the instructions therein.
- All information within the above-referenced ROC and in this attestation fairly represents the results of the assessment in all material respects.
- The Service Provider has read the PCI DSS and recognizes that they must maintain full PCI DSS compliance at all times.
- No evidence of magnetic stripe (i.e., track) data², CAV2, CVC2, CID, or CVV2 data³, or PIN data⁴ storage after transaction authorization was found on ANY systems reviewed during this assessment.

Part 3b. QSA and Service Provider Acknowledgments

	
Signature of Lead QSA ↑	Date: 01/Jun/2011
Lead QSA Name: Phil Kernick	Title: Information Security Professional
	
Signature of Service Provider Executive Officer ↑	Date: 01/Jun/2011
Service Provider Executive Officer Name: CHARLES GUTJAHR	Title: DIRECTOR OF IT

¹ "In place" results should include compensating controls reviewed by the QSA. If compensating controls are determined to sufficiently mitigate the risk associated with the requirement, the QSA should mark the requirement as "in place".

² Data encoded in the magnetic stripe used for authorization during a card-present transaction. Entities may not retain full magnetic stripe data after transaction authorization. The only elements of track data that may be retained are account number, expiration date, and name.

³ The three- or four-digit value printed on the signature panel or face of a payment card used to verify card-not-present transactions.

⁴ Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.